Regulación sobre protección de datos personales en el mundo digital en el Estado Colombiano.

Regulation on the protection of personal data in the digital world in the Colombian State.

Jesika Mercedes Barrera Campos [1]
Universidad Católica de Colombia

Resumen

La protección de datos personales en Colombia ha sido objeto de regulación a través de diversas normas y decretos que buscan fijar una serie de criterios para el manejo de la información personal de los individuos de modo que se garantice su privacidad y un uso adecuado de la misma de acuerdo con las disposiciones del titular. Ahora bien, teniendo en cuenta la era del comercio digital que se vive actualmente, como pregunta de investigación a desarrollar se ha planteado la siguiente: ¿El desarrollo normativo en Colombia sobre recolección y utilización de datos es idóneo para proteger la información de las personas que utilizan plataformas y canales digitales? Para ello se maneja como hipótesis principal, que la regulación en Colombia sobre protección de datos en la era digital hoy en día es insuficiente ya que existen criterios inciertos frente al manejo de estos datos y la responsabilidad que tienen las personas jurídicas que los recolectan.

***Palabras Clave*:** Colombia, Derecho a la intimidad, Derecho a la privacidad, Datos Personales, Comercio Digital, Plataformas digitales, Canales digitales.

Abstract

The protection of personal data in Colombia has been regulated through various rules and decrees that seek to set a series of criteria for the handling of personal information of individuals so that their privacy and proper use of it is guaranteed. in accordance with the

[1] Estudiante de Derecho con materias culminadas y en proceso de grado de la Universidad Católica de Colombia, identificado con código estudiantil N° 2110754. Correo electrónico: jmbarrera59@ucatolica.edu.do director Marco Emilio Sánchez Acevedo Docente e investigador de la Facultad de Derecho de la Universidad Católica de Colombia

provisions of the owner. Now, taking into account the era of digital commerce that is currently being lived, as a research question to be developed, the following has been asked: Is the regulatory development in Colombia on data collection and use suitable to protect the information of the people who Do you use digital channels and platforms? For this, it is handled as the main hypothesis, that the regulation in Colombia on data protection in the digital age today is insufficient since there are uncertain criteria regarding the handling of this data and the responsibility of the legal entities that collect it.

Key words: Colombia, Right to privacy, Right to privacy, Personal Data, Digital Commerce, Digital Platforms, Digital Channels.

Sumario

Introducción

Para comenzar, es importante indica que la privacidad e intimidad del ser humano, se ha considerado como una esfera esencial en la vida de estos, es por ello por lo que, desde la Declaración Universal de Derechos Humanos adoptada en París por la tercera Asamblea General de las Naciones Unidas, el 10 de diciembre de 1948 se hace referencia de manera explícita a aquellos los derechos y aquellas libertades de cada individuo, y la protección que debe darse a estos (Castro, 2016).

Ahora bien, dentro de los derechos contemplados en esta declaración, se encuentra precisamente el derecho a la intimidad que busca proteger la vida privada de cada individuo, esto dentro del conjunto de libertades que tiene el ser humano. En ese sentido, es importante que la normativa sobre el tema avance al compás de la tecnología, precisamente esta es la motivación principal, para la propuesta que aquí se ha planteado.

Lo anterior, tiene una incidencia tanto desde el aspecto académico, teniendo en cuenta que hace una evaluación de la normatividad existente para la protección de un derecho fundamental como lo es la privacidad e intimidad, y desde la aplicación del conocimiento adquirido evaluar la suficiencia de dicha normatividad, con la finalidad de formular recomendaciones.

Pero la utilidad de este, no se agota en el ámbito académico, sino que también trasciende al ámbito de la política pública, ya que a partir de la identificación de una problemática se pueden formular y planificar acciones para la solución de esta, por ello este análisis puede ser un insumo importante.

En ese orden de ideas, como pregunta de investigación a resolver con el presente artículo de reflexión, se ha planteado la siguiente ¿El desarrollo normativo en Colombia sobre recolección y utilización de datos es idóneo para proteger la información de las personas que utilizan plataformas y canales digitales? ello con el objetivo principal de Determinar si el desarrollo normativo en Colombia sobre protección de datos personales en el comercio digital es idóneo para la protección del derecho a la intimidad y privacidad de quienes utilizan canales y plataformas digitales.

Ahora bien, para alcanzar el objetivo principal se han planteado 3 objetivos específicos que responden al desarrollo de cada uno de los apartados de la investigación planteada. El primer apartado hace una descripción acerca de la normativa existente en Colombia sobre protección de datos personales, buscando establecer el desarrollo normativo sobre el tema en el país y su evolución. El segundo apartado se centra en evaluar los avances del comercio electrónico a través de plataformas y canales digitales, profundizando en estos conceptos, por último, el tercer apartado se centra en determinar si la regulación que en el momento existe en Colombia es idónea para garantizar a los usuarios del comercio digital la protección y utilización correcta de sus datos.

Metodología

La elaboración del artículo de investigación se realizará a partir de una línea de Investigación Jurídica documental, de naturaleza documental descriptiva que, a partir del análisis de

autores, jurisprudencia y pronunciamientos oficiales, busca construir una heurística que desarrolle el tema integralmente, permitiendo dar respuesta a la pregunta de investigación planteada (Agudelo, 2018).

1. La protección de datos personales como derecho fundamental.

Es necesario abordar en primer lugar el concepto de datos personales en el contexto del ordenamiento jurídico colombiano, para proceder a identificar la razón por la cual la protección de estos se considera como un derecho fundamental en sí mismo.

En ese sentido, como lo indica Rojas Bejarano (2014) los datos personales se entienden como la información de cualquier clase que se relacione de manera concreta con una persona. Bajo esta definición, es claro que este tipo de información tiene relación con la esfera de la vida privada de cada uno de los titulares de esta información.

Precisamente debido a lo anterior, como lo señala la Corte Constitucional, los primeros acercamientos del derecho a la protección de datos personales, se realizaron desde la percepción de una "garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable" (Corte Constitucional, Sentencia C-748 de 2011).

Esto en el entendido que desde la Constitución Política de 1991 se consagra el derecho a la intimidad de manera expresa en el artículo 15, advirtiendo el deber que tiene el Estado de respetar y hacer respetar este. Al respecto, menciona Herrán (2002) el alcance del derecho a la intimidad tiene un alcance esencial en la protección del desarrollo de individuo, por esto precisamente en Colombia el derecho a la protección de datos personales se relaciona en sus inicios de manera directa con el derecho a la intimidad.

Sin embargo, el alcance y la importancia de la protección de datos personales hizo que se generara en el ordenamiento jurídico colombiano una interpretación distinta, que considera el derecho al habeas data o protección de datos personales como un derecho fundamental autónomo.

En consecuencia, se reconoce que el derecho al habeas data tiene una serie de contenidos esenciales, los cuales se desarrollan por parte del máximo tribunal constitucional en Colombia, que estableció a través de su jurisprudencia lo siguiente:

> Dentro de las prerrogativas o contenidos mínimos que se desprenden del derecho al habeas data encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa.

Se observa en las aseveraciones de la Corte Constitucional la importancia de garantizar métodos adecuados para la recolección, administración, corrección y eliminación de datos personales en el ámbito precisamente de la garantía del derecho al habeas data de todos los individuos. Esto desde el reconocimiento de que es el titular de la información quien debe tomar las decisiones sobre quien tiene o no sus datos personales, y la forma en la cual se tratan los mismos.

En consecuencia, se hace necesario la expedición de una normativa específica que regule lo concerniente a la protección de datos personales en toda su extensión, siendo ello como lo advierte Torres Ávila (2016) una prioridad que el legislador tuvo que asumir ante la necesidad de dejar claras las reglas sobre el tema, y que las personas conozcan a que tienen derecho respecto de su información.

1.1 Normativa en Colombia sobre protección de datos personales:

En primer lugar, es indispensable indicar que desde la Constitución Política de Colombia en el Artículo 15 se hace referencia al derecho que tienen las personas de conocer, actualizar, retirar y rectificar cualquier tipo de información personal que se haya recolectado de estas,

así mismo se hace énfasis en que se deben respetar las garantías y libertades en este todos los procesos relacionados con datos personales.

Al respecto, Calle (2009) hace énfasis en que el desarrollo del artículo 15 de la Carta política ha estado en cabeza de la Corte Constitucional quien a través de su jurisprudencia ha desarrollado ampliamente los conceptos de datos personales y los derechos que del tratamiento de estos se derivan.

Ahora bien, en desarrollo del mandato constitucional, se presentaron varios proyectos de Ley que buscaban regular en su integridad la temática de tratamiento de datos personales, no obstante, dichos proyectos no tuvieron el suficiente apoyo y fueron archivados. Fue entonces hasta el año 2008 que se expidió la Ley 1266 de esta anualidad, como lo indica García (2015) esta norma tiene hace referencia al derecho de habeas data y el manejo de la informacion o datos personales en el sector financiero y crediticio.

Gil (2017) identifica a esta norma como esencial dentro de la identificación del derecho fundamental al habeas data, y la estructura que soporta todos los procesos de recolección de datos y tratamientos de la información. Esta norma plantea concretamente los derechos que tienen los titulares de la información, y los procedimientos que deben seguirse para hacer reportes negativos a centrales de riesgo, entre otros.

Años más tarde, se expide la Ley 1581 de 2012 cuyo ámbito de aplicación en esta ocasión es más extenso, Chaparro (2014) hace referencia a la importancia de los postulados que se definieron en esta norma, por ejemplo, la definición de los derechos de los titulares de la información de conocer, actualizar, rectificar, retirar sus datos personales de las bases de datos de empresas públicas y privadas.

Asi mismo, se fijan reglas importantes, por ejemplo, quien almacene y trate datos personales, debe contar con la autorización del titular a través de un medio valido (Galvis, 2012) y adicionalmente se deja por sentado que se debe informar al titular la forma en que se tratala la información y con qué finalidad se realizara. Es claro entonces, que esta norma abarca muchos más aspectos en materia de protección de datos que la Ley 1266 de 2008.

Por otro lado, en reglamentación de la Ley 1581 de 2012 se expidió el Decreto 1377 de 2013, esta norma señala expresamente que toda recolección de los datos personales debe darse en desarrollo de la finalidad de la persona natural o jurídica que los está recolectando, y salvo en los casos excepcionales previstos por la Ley, se debe contar con autorización expresa del titular de estos (Cubillos, 2017). De igual modo se establecen límites temporales para el almacenamiento de los datos, para lo cual deberá tenerse en cuenta el principio de razonabilidad y necesidad, esto como lo indica Sánchez (2015) en razón a la garantí del derecho a la intimidad, siendo este de carácter fundamental según la Constitución Política de 1991.

Es menester señalar también que la Superintendencia de Industria y Comercio ha desarrollado de manera amplia todos los aspectos que tienen que ver con protección de datos personales a través de unas guías que exponen de manera práctica las obligaciones que se han fijado para aquellas entidades públicas y privadas que sean responsables de la recolección y el tratamiento de datos personales.

En ese sentido, por ejemplo, la "Guía sobre el tratamiento de datos personales para fines de marketing y publicidad" creada por la Superintendencia de Industria y Comercio (2019) hace referencia a elementos indispensables para tener en cuenta en el marco de la protección de datos en el marco de las nuevas tecnologías de la información, comercio electrónico y marketing digital, una de las referencias más relevantes dentro de este documento es el concepto de responsabilidad demostrada.

Dicho concepto hace referencia a las medidas concretas que toman los responsables de la recolección y el tratamiento de datos personales frente a la protección de estos, en esa medida el ejercicio responsable de estas empresas o entidades públicas debe enmarcarse en la búsqueda de medidas necesarias, útiles, efectivas, oportunas y eficientes para que se cumplan las obligaciones legales que se tiene frente al derecho de habeas data.

En el marco de lo anterior, Recio (2017) ha mencionado que la responsabilidad demostrada es un principio fundamental en el marco de la protección de datos personales, considerando que a partir de este se puede asegurar que la recolección, tratamiento y transferencia de datos

personales se realiza bajo las normas que rigen el tema, pero además se toman las medidas efectivas orientadas a proteger los datos que se tienen de un individuo.

Es importante señalar que las guías desarrolladas por la Superintendencia de industria y comercio se han enfocado de manera específica en definir de acuerdo con la finalidad de la recolección de datos personales, las medidas que se deben tomar para proteger los mismos, así como los anexos y formatos para este ejercicio.

En este punto es necesario destacar que Colombia participo en la elaboración de los estándares de protección de datos personales de los Estados Iberoamericanos, los cuales en cierta medida compilan la normatividad que existe alrededor del tema y lo completan fijando principios aplicables, señalando temas puntuales como el derecho de indemnización y fijando criterios de cooperación internacional en la materia (Maqueo, Et al., 2017).

Ahora bien, en el marco de protección de datos personales en el marco del comercio electrónico no ha sido emitida una ley que concretamente se ocupe del tema, se ha hecho referencia a este tema en documentos CONPES sobre big data y comercio electrónico, y la Superintendencia de Industria y Comercio ha dado unas directrices sobre la manera en que se deben recolectar, almacenar y gestionar los datos personales de los usuarios de canales y plataformas electrónicas.

En ese sentido, en la guía mencionada anteriormente la Superintendencia de Industria y Comercio (2020) menciona la importancia de que cada uno de los actores que participa en la cadena de valor de una transacción de comercio electrónico entre a evaluar los datos a los que tendrá acceso en virtud de esta y defina las medidas necesarias para garantizar una recolección y tratamiento seguros.

Para lo anterior, se hace necesario que se evalúen los riesgos que se tienen en el marco del proceso de recolección y tratamiento, y es esencial que se ciñan a los principios que se mencionan a continuación en la figura 1.

Figura 1. Principios aplicables en materia de tratamiento de datos para comercio electrónico. Fuente: Superintendencia de Industria y Comercio (2019).

En ese sentido, resulta claro que los usuarios de comercio electrónico tienen una serie de garantías respecto de la protección de datos personales, y ello debe ser garantizado por cada uno de los actores de la transacción realizada en el marco de comercio electrónico, utilizando los mismos únicamente para el fin previsto y que se le ha indicado al usuario.

No obstante, no se ha regulado el tema a través de una Ley propiamente, como si se ha hecho en otros países, y como lo advierte Monsalve (2017) "es evidente que se requiere de regulación sectorial para la correcta aplicación del habeas data informático" (p.192), esto debido a la particularidad del sector de comercio electrónico, de hecho, varios países en la actualidad han regulado el tema de manera satisfactoria, dichos ejemplos que se analizaran a continuación.

2. Datos personales en el comercio electrónico y canales digitales.

Es importante destacar que el avance en materias de tecnología de la información ha generado que las transacciones comerciales migren hacia nuevos escenarios como el digital. En consecuencia, el comercio electrónico se ha fortalecido en los últimos años, con la aparición

de nuevas herramientas como plataformas de pagos, e incluso la integración de espacios de compras en redes sociales de frecuente utilización.

Por ello, con el fin de entender la dinámica de este tipo de relación comercial, se busca hacer unas precisiones en cuanto a este tipo de comercio, en el mundo negocial.

2.1 Generalidades del comercio electrónico:

Inicialmente es importante señalar que el comercio electrónico se concibe como "la compra y venta de productos o de servicios a través de medios electrónicos, principalmente internet y otras redes de datos" (Comisión de regulación de Comunicaciones, 2017, p.27), otra de las definiciones para este término acotada por la OCDE que denomina a esta clase de comercio como cualquier transacción que tenga como finalidad venta de bienes o servicios y se efectué a través de redes de computadores por medio de métodos o plataformas para procesar pagos (OCDE, 2013).

Es preciso entonces, señalar que existen diversas modalidades de comercio electrónico, las cuales deben su clasificación a los agentes que participan en la relación comercial. Así entonces, hay comercio electrónico entre empresas que se conoce comúnmente como relaciones Business to Business (B2B) y hacen referencia en este campo a aquellas transacciones electrónicas que se dan entre empresas (Kotler & Pfoertsch, 2007).

Por otra parte, existe también una modalidad de comercio electrónico que se presenta entre empresas y consumidores, que se conoce como relaciones *Business to Consumer o* B2C, generalmente estas se dan a través de páginas web o aplicaciones móviles que diseñan y administran las empresas. Otra de las categorías reconocidas en el marco de esta actividad son aquellas relaciones que se presentan entre empresas y el Estado, generalmente ello se da en el marco de la contratación estatal, en la adquisición de bienes o servicios.

Como lo señalan Sarmiento, Mariño y Forero (2015) la contratación pública electrónica es una modalidad que se ha venido implementando en varios Estados, entre ellos Colombia quien ha diseñado plataformas como SECOP I y II a través de las cuales se manejan los procesos de contratación o la Tienda virtual del Estado colombiano que es un mecanismo de

agregación de demanda, diseñado para las compras en masa a través de proveedores definidos por el Estado, todas estas manejadas a través de Colombia Compra Eficiente.

De igual modo también se han diseñado plataformas que permiten a los consumidores hacer transacciones entre sí, en la mayoría de estos casos las condiciones de la transacción se dejan al arbitrio de las partes negociales, este tipo de comercio electrónico se conoce como relaciones Consmer to Consumer o C to C (Ríos, 2014). Hechas las precisiones anteriores, se muestra a continuación la figura 1 que permite observar algunos ejemplos de plataformas y páginas web, que se destacan en cada una de las modalidades de comercio electrónico.

Figura 1. Modalidades de comercio electrónico. Fuente: Unión Temporal RocaSalvatella – Infométrika.

En esa medida, es claro que el comercio electrónico es la transacción o relación negocial que se presenta a través de medios o canales digitales, que como se evidencia en la gráfica anterior se materializa a través de una serie de plataformas dispuestas para tal fin.

Es menester indicar que dicha transacción requiere de la intervención de varios actores, ello se conoce como la cadena de valor en el comercio electrónico, lo cual resulta relevante para el objeto de estudio del presente artículo a fin de definir las responsabilidades de cada actor frente a los datos personales de quienes utilizan estas plataformas, por ello el tema será tratado a continuación.

2.2 Actores en la cadena de las transacciones de comercio electrónico:

Como se mencionó anteriormente, las transacciones en el marco del comercio electrónico integran varios actores de principio a fin, ello concretamente debido a que la plataforma o página web que inicialmente ofrece el bien o servicio, debe contar con servicios adicionales para el pago, envío, entre otros.

Como lo indica Herreros (2019) uno de los actores principales en el comercio electrónico son plataformas digitales, estas se encargan de reunir a compradores y vendedores de bienes o servicios en un mismo espacio que se denomina mercado virtual, ejemplo de estas plataformas que son mundialmente reconocidas son Amazon, E-bay, Mercado Libre, entre otros.

Como lo advierte Cruz (2018) este tipo de plataformas se ha fortalecido en el mercado debido a las ventajas que se generan respecto de los costos de operación que representa una tienda física, adicionalmente el reunir proveedores de varios bienes y servicios permite que se genere un importante reconocimiento por parte de los consumidores de este tipo de plataformas.

No obstante, las plataformas deben actuar de manera mancomunada con otros canales como plataformas de pago, servicios de mensajería, entre otros. Lo anterior, se evidencia de manera más precisa en la figura 2 que se muestra a continuación.

Figura 2. Cadena de Valor en materia de comercio electrónico.

Como se puede observar en la figura anterior, son varios los actores que tienen algún tipo de función respecto de las transacciones de comercio electrónico, ello en el entendido que deben surtirse varios pasos desde la compra del producto por parte del comprador, hasta la entrega de este.

Es importante en este punto señalar que respecto de las responsabilidades del proveedor en materia de comercio electrónico la Corte Constitucional se pronunció de la siguiente manera:

> Dado que la definición legal de proveedor implica llevar a cabo habitualmente tales operaciones, si el productor también se encarga de comercializar sus productos y emplea, directa o indirectamente, mecanismos electrónicos para el efecto, fungirá también como proveedor y la norma extenderá a él sus obligaciones y responsabilidades en materia de seguridad de los dispositivos utilizados (Corte Constitucional colombiana, Sentencia C-439 de 2019)

Lo anterior, podría dar a entender que en cabeza del proveedor se encuentra la responsabilidad total de la recolección, tratamiento y almacenamiento de datos personales, que es una de las responsabilidades en materia de comercio electrónico, sin embargo, esto no es específico en el pronunciamiento. Es por ello, que existe la necesidad de una normativa

clara que asigne responsabilidades a cada uno de estos actores respecto del tratamiento de datos personales, y el almacenamiento de estos, se genera una mayor eficacia respecto de la vigilancia y control del derecho de habeas data de los usuarios que realizan transacciones por medios electrónicos.

Es importante en este punto mencionar, que la Superintendencia de Industria y Comercio en el contexto colombiano ha tenido que entrar a analizar cuando una empresa tiene un rol determinado y cuando es un intermediario como tal, como es el caso de Rappi, en el cual indicó:

> RAPPI S.A.S. no funge como portal de contacto, sino que actúa como una plataforma de comercio electrónico, en la medida en que es parte de la cadena de comercialización de los bienes y servicios que ofrece y obtiene un porcentaje de las operaciones realizadas a través de sus plataformas. Realiza de manera directa propaganda comercial con inventivos a través de mensajes de texto que son enviados a los consumidores. Tiene a su cargo la emisión y difusión exclusiva de piezas publicitarias en sus plataformas (Superintendencia de Industria y Comercio, Resolución 40212 de 2019).

Lo anterior lo realizo con el fin de especificar cuáles son las responsabilidades que tiene Rappi con los usuarios que utilizan este canal, dejando claro que se considera una plataforma de comercio electrónico y en consecuencia sus términos y condiciones deben estar ajustados a ello, de manera que no todos los actores cuentan con las mismas obligaciones de cara al consumidor o usuario.

En el caso de Colombia, se observa que, si bien existen lineamientos generales, hoy las disposiciones de la Ley 1581 de 2012 se quedan cortas respecto de los avances en materia de tecnologías de la información y comercio electrónico. Si bien es cierto que han existido sanciones por la indebida utilización de datos personales recolectados en transacciones electrónicas, las mismas se enmarcan en la vulneración de la legislación existente que podría presentarse o no en materia de comercio electrónico.

Esto en el entendido de que en la cadena de valor del comercio electrónico existen muchos actores que tienen acceso a información personal del usuario, lo cual es esencial para el desarrollo de su actividad dentro de la cadena de valor, sin embargo, también es necesario definir en primer lugar que tipo de información requiere el actor de acuerdo al eslabón que representa en la cadena de valor, en segundo lugar es importante que el usuario conozca la forma en la cual se tratan y almacenan sus datos desde la compra en la plataforma, a fin de que exista conocimiento efectivo de a dónde llega esta información para posteriormente poder ejercer cualquiera de las acciones relacionadas con el derecho de habeas data.

Posterior al ejercicio de reconocimiento de generalidades y cadena de valor en el ámbito de comercio electrónico, es necesario entrar a determinar la idoneidad de la normativa que existe en Colombia frente al tratamiento de datos personales en el ámbito de las transacciones que son realizadas a través de comercio electrónico. Para ello, se hará referencia específica a la forma en que se abordado el tema en Colombia, y se hará una descripción sucinta de experiencias internacionales en este ámbito.

3. Idoneidad de la regulación colombiana en cuanto a protección de datos en comercio y canales digitales

Como se mencionó en los capítulos anteriores en Colombia existen una normativa respecto de la protección de datos personales, esta contempla de manera general los deberes de aquellas entidades tanto públicas como privadas respecto del tratamiento, gestión y almacenamiento de datos personales, así como los derechos de los titulares de este tipo de información.

En ese sentido, las obligaciones de los responsables de tratamiento de datos personales como conservar prueba de la autorización del titular, crear un política de protección de datos personales que sea pública, documentar los procedimientos que se siguen respecto de la protección de datos, entre otros, aplican también para aquellas plataformas y empresas que realizan actividades de comercio electrónico, y los terceros que obren en nombre de este, ello de acuerdo a la guía que ha establecido la Superintendencia de Industria y Comercio (2017) en materia de protección de datos en el comercio electrónico.

No obstante, no existe en la actualidad una norma específica que a través de la identificación de la cadena de valor de las transacciones de comercio electrónico establezca responsabilidades para todos los actores, ni tampoco se evidencia un procedimiento de inspección vigilancia y control para este tema concreto, lo que sin duda deja a la deriva aspectos fundamentales frente a la regulación en el ámbito específico del comercio electrónico (Newman y Ángel, 2018).

Si bien es cierto, que existen artículos en diversas normas como el estatuto del consumidor, u otras sobre identificación electrónica, lo cierto es que ellas no se encuentran de manera específica compiladas en una norma o decreto que regule lo concerniente al tema de protección de datos en el ámbito del comercio electrónico, son normas dispersas que están en el ordenamiento jurídico colombiano y regulan otras materias distintas al comercio electrónico.

También es esencial destacar que entendiendo la importancia de emitir una regulación concreta en materia de comercio electrónico en 2010 se aprobó el Documento CONPES 3620 sobre "Lineamientos de política para el impulso del comercio electrónico en Colombia" que se centra concretamente en acciones para fomentar el desarrollo de este tipo de comercio en Colombia, en este se advierte que existen vacíos normativos frente al tema, y también una serie de barreras que impiden el posicionamiento de plataformas y canales digitales.

Posteriormente, en el año 2019 se profirió el Documento CONPES 3975 denominado "Política nacional para la transformación digital e inteligencia artificial" que introduce algunas nociones sobre la cadena de valor del comercio electrónico, sin centrarse específicamente en la regulación necesario para proteger a los extremos que intervienen en la transacción electrónica (Martínez, 2019).

Así mismo, en junio del año 2020 se publicó un borrador de Documento CONPES sobre comercio electrónico, esto a consecuencia de las debilidades en la materia evidenciada por los denominados "días sin IVA", que dieron cuenta de la insuficiencia de las plataformas electrónicas cuando existe un alto tráfico de usuarios en la misma. Sin embargo, frente a la protección de datos personales en este ámbito no se ha evidenciado una verdadera preocupación. Ahora bien, dicho lo anterior es importante hacer referencia en este punto a

experiencias internacionales que han regulado específicamente el tema de protección de datos personales en el comercio electrónico.

El primer ejemplo que se observa es la regulación sobre la obtención y tratamiento de datos en canales y plataformas digitales, al respecto Castaños y Castillo (2019) señalan que la primera forma de proteger la información es fijar un Reglamento General de Protección de Datos (Reglamento [UE] 2016/679) que entra en vigencia en el año 2018, este regula aspectos como la necesidad de autorización para la recolección de información a través de Cookies que se instalan en dispositivos electrónicos, así mismo se advierte que cuando las empresas hagan cambios en sus políticas de privacidad deberán notificar a aquellas personas de quienes tienen datos personales almacenados y estas deben autorizar el tratamiento de sus datos bajo esta nueva política.

Así mismo se establece que únicamente se podrán tratar los datos con una finalidad especifica que sería previamente informada al titular, y en todo caso se debe contar con su consentimiento explícito para ello. También, se advierte que deben realizarse procedimientos sencillos para que se solicite la baja de la información por parte de los titulares.

El segundo ejemplo que se trae de referencia es la Ley de Privacidad del Consumidor de California, esta como lo advierte Porcelli (2020) esta norma busca darles a los consumidores un control real sobre su información personal, dotándolos de la capacidad para solicitar que se eliminen sus datos en cualquier momento y generando sanciones ejemplares (multas) a aquellas empresas que no atiendan la solicitud.

Es esencial indicar que Colombia ha hecho un gran esfuerzo para regular las responsabilidades de los actores que participan en el comercio electrónico respecto del tratamiento de datos personales, siendo los documentos CONPES, las guias de la Superintendencia de Industria y Comercio, entre otros elementos esenciales en la materia, es evidente que hace falta regular el tema desde el aspecto normativo específicamente.

Lo anterior, en cuanto es claro que la normatividad expedida hasta la fecha en materia de protección de datos personales se pensó en otro momento histórico donde si bien habían avances en materia tecnológica no era visible la importancia que tomarían las tecnologías de

la información en materia de comercio electrónico, lo que hace necesario que la legislación avance a medida que la tecnología lo hace, para no quedar relegados en escenarios de inseguridad jurídica respecto de situaciones concretas.

Conclusiones

1. Como se ha evidenciado en el presente artículo de reflexión las tecnologías de la información avanzan de manera acelerada alrededor del mundo, generando nuevas alternativas para consumidores y usuarios respecto de la adquisición de bienes y servicios. En el marco de lo anterior precisamente el comercio electrónico ha venido posesionándose como una manera ágil y rápida de realizar compras que anteriormente requerían la presencialidad del comprador en un punto de venta.
2. Es importante mencionar en este sentido que el comercio electrónico implica una serie de pasos que involucran a diversos agentes y actores, desde el primer paso donde se produce la selección y pago del bien o servicio hasta la entrega de este en el lugar de destino señalado por el comprador. Debido a esta situación los datos personales de los usuarios o consumidores son recolectados por diferentes actores, lo que hace indispensable que estén claras las reglas sobre el tratamiento de estos datos y su almacenamiento.
3. Si bien en Colombia se han adaptado las normas existentes para transacciones y comercio electrónico hoy en día no existe una regulación específica que defina responsabilidades de los actores de los canales electrónicos, pasarelas de pago, empresas de mensajería, entre otros que participan en la cadena de valor de la transacción electrónica y por lo tanto recolectan y almacenan los datos personales de usuarios y consumidores.
4. Así mismo, hay temas específicos como el alcance de la autorización del usuario o consumidor sobre el tratamiento de sus datos en transacciones de comercio electrónico, en ese sentido existen dudas sobre si esta autoriza a todos los actores de la cadena a tratar y almacenar sus datos o si por el contrario deberían usarse únicamente en el marco de la transacción de comercio electrónico y darse de baja de manera inmediata.

5. Así entonces, si bien es cierto en Colombia se han generado pautas para la protección de datos en materia de comercio electrónico a la fecha, la misma resulta insuficiente ya que no tiene un respaldo normativo que trate de manera específica el tema y haya analizado en consecuencia los escenarios de riesgos y responsabilidades de los intervinientes de transacciones en materia de comercio electrónico. Esta situación que hace necesario que el legislador se involucre en este tema y lo estudio de manera amplia a fin de regularlo, para lo cual es procedente acudir a las reglas establecidas en otros Estados.

Referencias.

Agudelo, Ó. A. (2018). Los calificativos del derecho en las formas de investigación jurídica. En Ó. A. Agudelo-Giraldo, J. E. León Molina, M. A. Prieto Salas, A. Alarcón-Peña & J. C. Jiménez-Triana. La pregunta por el método: derecho y metodología de la investigación (pp. 17-44). Bogotá: Universidad Católica de Colombia.

Calle, S. B. (2009). Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia. Precedente. Revista Jurídica, (-), 119-136. https://doi.org/10.18046/prec.v0.1459

Chaparro, M. F. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. INVENTUM, 9(17), 32-37.

Comisión de Regulación de Comunicaciones. (2017). El comercio electrónico en Colombia: análisis integral y perspectiva regulatoria. Documento soporte, versión Online: https://www.crcom.gov.co/recursos_user/2017/ComElecPtd_0.pdf

Cruz, I. (2018). Innovación, cambio y competitividad en el comercio. Distribución y Consumo, 28(151), 31-34.

Cubillos, Á. (2017). La explotación de los datos personales por los gigantes de internet. Estudios en derecho a la información, (3), 27-55.

García Vargas, C. (2015). La incidencia del modelo español en el registro nacional de bases de datos colombiano como herramienta de supervisión y control. En: J. Becerra, G. D. Flórez Acero, C. García Vargas, C. Rojas Orjuela Vargas, M. E. Sánchez Acevedo & J. Torres Ávila. El derecho y las tecnologías de la información y la comunicación (TIC) (pp. 101-160). Bogotá: Universidad Católica de Colombia.

Galvis, L. (2012). Protección de datos en Colombia, avances y retos. Revista Lebret, 4(4), 195-214. Recuperado de http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336

Gil, C. (2017). El debido proceso en la Ley de Habeas Data. Rev. CES Derecho., 8(1), 191-204.

Herrán, A. I. (2002). El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales. Librería Editorial Dykinson.

Herreros, S. (2019). La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe. Informe CEPAL comercio internacional.

Kotler, P., & Pfoertsch, W. (2007). Being known or being one of many: the need for brand management for business-to-business (B2B) companies. Journal of Business & Industrial Marketing, 22(6), 357-362.

Maqueo, M. S., Moreno, J., & Recio, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Revista de derecho (Valdivia), 30(1), 77-96.

Martinez Devia, A. (2019). La Inteligencia Artificial, el Big Data y la Era Digital: Una Amenaza para los Datos Personales. Rev. Prop. Inmaterial, 27, 5.

Monsalve Caballero, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. Prolegómenos. Derechos y Valores, XX (39),163-195. ISSN: 0121-182X.

Recio, M. (2017). Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, (17), 3.

Ríos, A. (2014). Análisis y perspectivas del comercio electrónico en México. Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento, 11 (1), 97-121

Rojas Bejarano M. (2014). Evolución del derecho de protección de datos personales en colombia respecto a estándares internacionales. Novum Jus, 8(1), 107-139. https://doi.org/10.14718/NovumJus.2014.8.1.6

Sánchez Acevedo, M. E. (2015). El régimen de responsabilidad de la Administración Pública colombiana por la publicación de contenidos mediante el uso de las tecnologías de la información y comunicación (TIC). En: J. Becerra, G. D. Flórez Acero, C. García Vargas, C. Rojas Orjuela Vargas, M. E. Sánchez Acevedo & J. Torres Ávila. El derecho y las tecnologías de la información y la comunicación (TIC) (pp. 15-38). Bogotá: Universidad Católica de Colombia.

Sarmiento, J., Mariño, C., & Forero, C. (2015). La contratación administrativa electrónica. Revista Civilizar Ciencias Sociales y Humanas, 15(29), 31-58.

Superintendencia de Industria y Comercio. (2019). Guía sobre el tratamiento de datos personales para fines de marketing y publicidad. Delegatura Para La Protección De Datos Personales. Publicación Oficial.

Superintendencia de Industria y Comercio. (2019). Guía sobre el tratamiento de datos personales para fines de marketing y publicidad. Delegatura Para La Protección De Datos Personales. Publicación Oficial.

Torres Ávila, J. (2016). Estrategias de implementación de las obligaciones del derecho de acceso a la información pública y la transparencia en el ámbito local. En J. Torres Ávila. La transparencia y el buen gobierno: una perspectiva desde los derechos humanos y las obligaciones de los gobiernos locales (pp. 89-104). Bogotá: Universidad Católica de Colombia.

Jurisprudencia

Corte Constitucional colombiana. (2011). Sentencia C-748 de octubre 6. M.P Jorge Ignacio Pretelt Chaljub.

Corte Constitucional colombiana. (2019) Sentencia C-429 de septiembre 25. M.P Diana Fajardo Rivera.